Network Working Group
Internet-Draft
Updates: 7489 (if approved)
Intended status: Informational
Expires: April 28, 2019

S. Kitterman
fTLD Registry Services

October 25, 2018

DMARC (Domain-based Message Authentication, Reporting, and Conformance) Extension For PSDs (Public Suffix Domains)

draft-kitterman-dmarc-psd-00

Abstract

DMARC (Domain-based Message Authentication, Reporting, and Conformance) is a scalable mechanism by which a mail-originating organization can express domain-level policies and preferences for message validation, disposition, and reporting, that a mail-receiving organization can use to improve mail handling. DMARC policies can be applied at the individual domain level or for a set of domains at the organizational level. The design of DMARC precludes grouping policies for a set of domains above the organizational level, such as TLDs (Top Level Domains). These types of domains (which are not all at the top level of the DNS tree) can be collectively referred to as Public Suffix Domains (PSDs). For the subset of PSDs that require DMARC usage, this memo describes an extension to DMARC to enable DMARC functionality for such domains.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

DMARC [RFC7489] provides a mechanism for publishing organizational policy information to email receivers. DMARC [RFC7489] allows policy to be specified for both individual domains and sets of domains within a single organization. For domains above the organizational

level in the DNS tree, policy can only be published for the exact domain. There is no method available to such domains to express lower level policy or receive feedback reporting for sets of domains. This prevents policy application to non-existent domains and identification of domain abuse in email, which can be important for brand and consumer protection.

As an example, imagine a country code TLD (ccTLD) which has public subdomains for government and commercial use (.gov.example and .com.example). Within the .gov.example public suffix, use of DMARC [RFC7489] has been mandated and .gov.example has published its own DMARC [RFC7489] record:

"v=DMARC1;p=reject;rua=mailto:dmarc@dmarc.service.gov.example"

at

_dmarc.gov.example.

This would provide policy and feedback for mail sent from @gov.example, but not @tax.gov.example and there is no way to publish an organizational level policy that would do so. While, in theory, receivers could reject mail from non-existent domains, not all receivers do so. Non-existence of the sending domain can be a factor in a mail delivery decision, but is not generally treated as definitive on its own.

This memo provides a simple extension to DMARC [RFC7489] to allow operators of Public Suffix Domains (PSDs) to express policy for groups of subdomains, extends the DMARC [RFC7489] policy query functionality to detect and process such a policy, describes receiver feedback for such policies, and provides controls to mitigate potential privacy considerations associated with this extension.

There are two types of Public Suffix Operators (PSOs) for which this extension would be useful and appropriate:

- Branded PSDs (e.g., ".google"): These domains are effectively Organizational Domains as discussed in DMARC [RFC7489]. They control all subdomains of the tree. These are effectively private domains, but listed in the Public Suffix List. They are treated as Public for DMARC [RFC7489] purposes. They require the same protections as DMARC [RFC7489] Organizational Domains, but are currently excluded.

- Multi-organization PSDs that require DMARC usage (e.g., ".bank"): Because existing Organizational Domains using this PSD have their own DMARC policy, the applicability of this extension is for non-

existent domains. The extension allows the brand protection benefits of DMARC [RFC7489] to extend to the entire PSD, including cousin domains of registered organizations.

Due to the design of DMARC [RFC7489] and the nature of the Internet email architecture [RFC5598], there are interoperability issues associated with DMARC [RFC7489] deployment. These are discussed in Interoperability Issues between DMARC and Indirect Email Flows [RFC7960]. These issues are not applicable to PSDs, since they (e.g., the ".gov.example" used above) do not send mail.

DMARC [RFC7489], by design, does not support usage by PSD operators. For PSDs that require use of DMARC [RFC7489], an extension of DMARC reporting and enforcement capability is needed for PSD operators to effectively manage and monitor implementation of PSD requirements.

2. Terminology and Definitions

This section defines terms used in the rest of the document.

2.1. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2.2. Public Suffix Domain (PSD)

The global Internet Domain Name System (DNS) is documented in numerous Requests for Comment (RFC). It defines a tree of names starting with root, ".", immediately below which are Top Level Domain names such as ".com" and ".us". They are not available for private registration. In many cases the public portion of the DNS tree is more than one level deep. PSD DMARC includes all public domains above the organizational level in the tree, e.g., ".gov.uk".

2.3. Longest PSD

Organizational Domain (DMARC [RFC7489] Section 3.2) with one label removed.

2.4. Public Suffix Operator (PSO)

A Public Suffix Operator manages operations within their PSD.

2.5. PSO Controlled Domain Names

PSO Controlled Domain Names are names in the DNS that are managed by a PSO and are not available for use as Organizational Domains (the term Organizational Domains is defined in DMARC [RFC7489] Section 3.2). Depending on PSD policy, these will have one (e.g., ".com") or more (e.g., ".co.uk") name components.

2.6. Non-existent Domains

For DMARC [RFC7489] purposes, a non-existent domain is a domain name that publishes none of A, AAAA, or MX records that the receiver is willing to accept. This is a broader definition than that in NXDOMAIN [RFC8020].

3. PSD DMARC Updates to DMARC Requirements

This document updates DMARC [RFC7489] as follows:

3.1. General Updates

References to "Domain Owners" also apply to PSOs.

3.2. Section 6.1 DMARC Policy Record

PSD DMARC records are published as a subdomain of the PSD. For the PSD ".example", the PSO would post DMARC policy in a TXT record at "_dmarc.example".

3.3. Section 6.5. Domain Owner Actions

In addition to the DMARC [RFC7489] domain owner actions, PSOs will need to update the "DMARC Public Suffix Domain (PSD) Registry". This registry is defined in Section 6.1.

3.4. Section 6.6.3. Policy Discovery

A new step between step 3 and 4 is added:

3A. If the set is now empty and the longest PSD (Section 2.3) of the Organizational Domain is listed in the DMARC PSD Registry (defined in Section 6.1), the Mail Receiver MUST query the DNS for a DMARC TXT record at the DNS domain matching the longest PSD (Section 2.3) in place of the RFC5322.From domain in the message (if different). A possibly empty set of records is returned.

As an example, for a message with the Organizational Domain of "example.compute.cloudcompany.com.cctld", the query for PSD DMARC

would use "compute.cloudcompany.com.cctld" as the longest PSD (Section 2.3). The receiver would check to see if that PSD is listed in the DMARC PSD Registry, and if so, perform the policy lookup at "_dmarc.compute.cloudcompany.com.cctld".

Note: Because the PSD policy query comes after the Organizational Domain policy query, PSD policy is not used for Organizational domains that have published a DMARC [RFC7489] policy. Specifically, this is not a mechanism to provide feedback addresses (RUA/RUF) when an Organizational Domain has declined to do so.

3.5. Section 7. DMARC Feedback

Operational note for PSD DMARC: For PSOs, feedback for non-existent domains is desired and useful. Because of the constraints on PSD DMARC scope, there are no significant privacy considerations associated with this reporting (See Section 4).

4. Privacy Considerations

This document does not significantly change the Privacy Considerations of [RFC7489].

4.1. Feedback leakage

Providing feedback reporting to PSOs can, in some cases, create leakage of information outside of an organization to the PSO. There are roughly three cases to consider:

- Branded PSDs (e.g., ".google"), RUA and RUF reports based on PSD DMARC have the potential to contain information about emails related to entities managed by the organization. Since both the PSO and the Organizational Domain owners are common, there is no privacy risk for either normal or non-existent Domain reporting.

- Multi-organization PSDs that require DMARC usage (e.g., ".bank"): PSD DMARC based reports will only be generated for domains that do not publish a DMARC policy at the organizational or host level. For domains that do publish the required DMARC policy records, the feedback reporting addresses (RUA and RUF) of the organization (or hosts) will be used. Since PSD DMARC is limited to PSDs that mandate Organizational Domains publish DMARC policy for existing domains, the risk of this issue is limited to Organizational Domains that are out of compliance with PSD policy.

- Multi-organization PSDs (e.g., ".com") that do not mandate DMARC usage. Privacy risks for Organizational Domains within such PSDs would be significant. This is mitigated by the limitation to only

include PSDs listed in the public IANA DMARC PSD Registry described in Section 6.1.

PSOs will receive feedback on non-existent domains, which may be similar to existing Organizational Domains. Feedback related to such cousin domains have a small risk of carrying information related to an actual Organizational Domain. To minimize this potential concern, PSD DMARC feedback is best limited to Aggregate Reports. Feedback Reports carry more detailed information and present a greater risk.

5. Security Considerations

This document does not change the Security Considerations of [RFC7489].

6. IANA Considerations

This section describes actions requested to be completed by IANA.

6.1. DMARC Public Suffix Domain (PSD) Registry

IANA is requested to create a new DMARC Public Suffix Domain (PSD) Registry within the Domain-based Message Authentication, Reporting, and Conformance (DMARC) Parameters Registry.

Names of PSDs participating in PSD DMARC must be registered with IANA in this new sub-registry. New entries are assigned only for PSDs that require use of DMARC. The requirement has to be documented in a manner that satisfies the terms of Expert Review, per [RFC5226]. The Designated Expert needs to confirm that provided documentation adequately describes PSD policy to require domain owners to use DMARC or that all domain owners are part of a single organization with the PSO.

The initial set of entries in this registry is as follows:

PSD	Reference	Status
.bank	this document	current
.insurance	this document	current
.gov.uk	this document	current

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7489] Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, DOI 10.17487/RFC7489, March 2015, <https://www.rfc-editor.org/info/rfc7489>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

7.2. Informative References

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 5226, DOI 10.17487/RFC5226, May 2008, <https://www.rfc-editor.org/info/rfc5226>.

[RFC5598] Crocker, D., "Internet Mail Architecture", RFC 5598, DOI 10.17487/RFC5598, July 2009, <https://www.rfc-editor.org/info/rfc5598>.

[RFC7960] Martin, F., Ed., Lear, E., Ed., Draegen. Ed., T., Zwicky, E., Ed., and K. Andersen, Ed., "Interoperability Issues between Domain-based Message Authentication, Reporting, and Conformance (DMARC) and Indirect Email Flows", RFC 7960, DOI 10.17487/RFC7960, September 2016, <https://www.rfc-editor.org/info/rfc7960>.

[RFC8020] Bortzmeyer, S. and S. Huque, "NXDOMAIN: There Really Is Nothing Underneath", RFC 8020, DOI 10.17487/RFC8020, November 2016, <https://www.rfc-editor.org/info/rfc8020>.

Acknowledgements

TBS

Author's Address

Scott Kitterman
fTLD Registry Services
600 13th Street, NW, Suite 400
Washington, DC 20005
United States of America

Phone: +1 301 325-5475
Email: scott@kitterman.com